

The Futures Circle – Presenting a framework for Hermeneutic TA to deconstruct technofutures of Quantum Computing

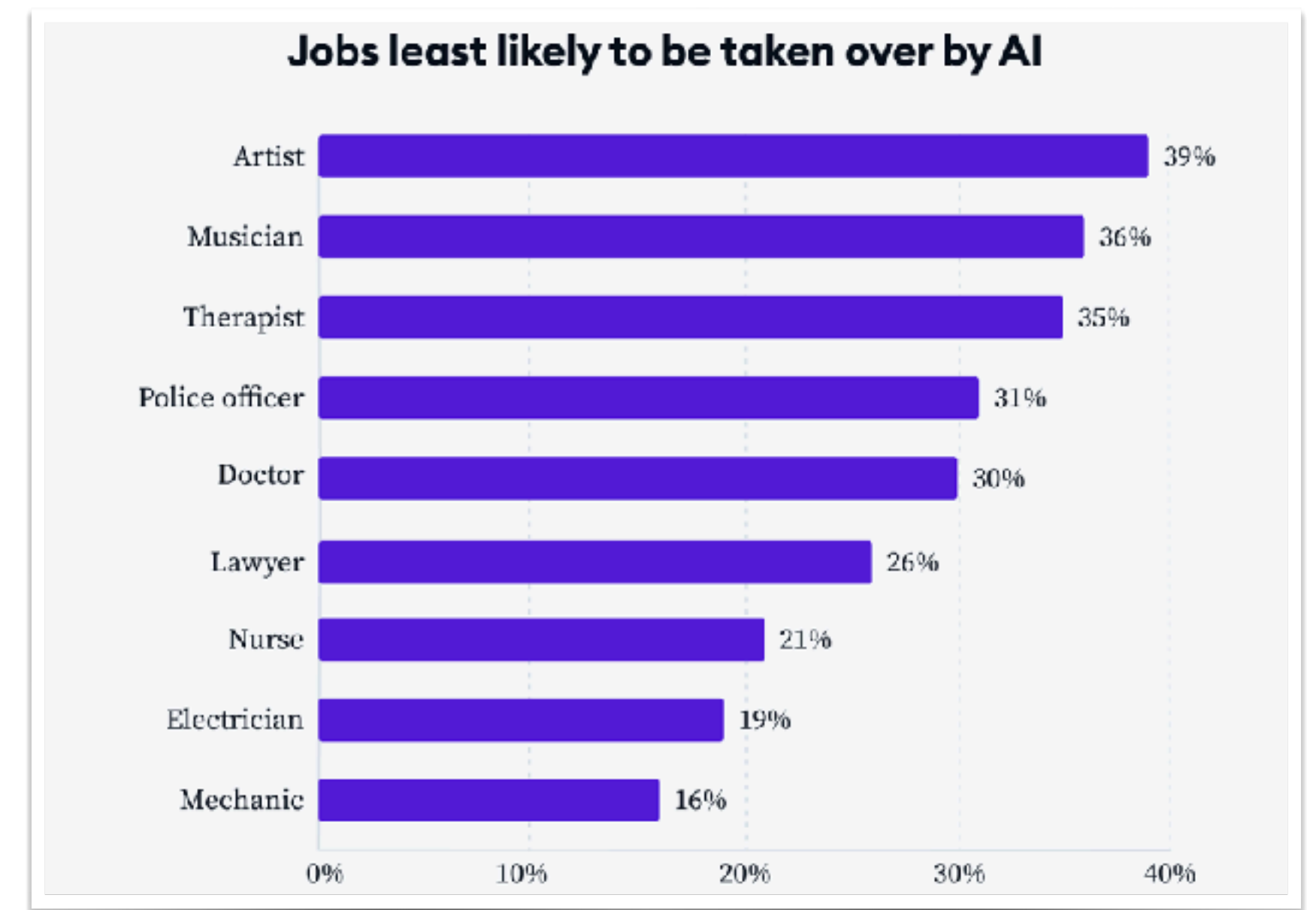
Wenzel Mehnert (cultural studies, future studies, hypestudies.org)
Technology Foresight, **Austrian Institute of Technology**
Philosophy of Technology, **TU Berlin**

Future Studies
as
Imaginary Studies

Technofutures

Technofutures are...

- ▶ ... **mediated statements** about our world being changed by new sciences or **technologies**, at a time when these technologies **have not yet materialised**.
- ▶ They come in the form of presentations, foresight reports, science fiction narratives, advertising, corporate visions, etc.



If-and-then statement (Nordmann, 2007)

- ▶ Narratives of causal change
- ▶ **If**: Function of an emergent technology
- ▶ **Then**: Promised / expected change that occurs through the function

- ▶ **If** we can create a direct interface between brains and machines
then this would be an invasion of privacy (Nordmann, 2007).

- ▶ Often, neither the **if** nor the **then** can be claimed with certainty.
- ▶ Discussion often circle around the **then** and ignore the feasibility of **if** (#speculative ethics; #hype)

Societal meaning

- ▶ Technofutures attribute societal meaning to an emerging technology.
- ▶ **Then:** Ethical, cultural, economic, social, political or ecological changes (Lösch et al., 2016).
- ▶ Emerging technologies become socially meaningful and require actors to **position themselves** in relation to the alleged changes (Grunwald, 2019, p. 105).



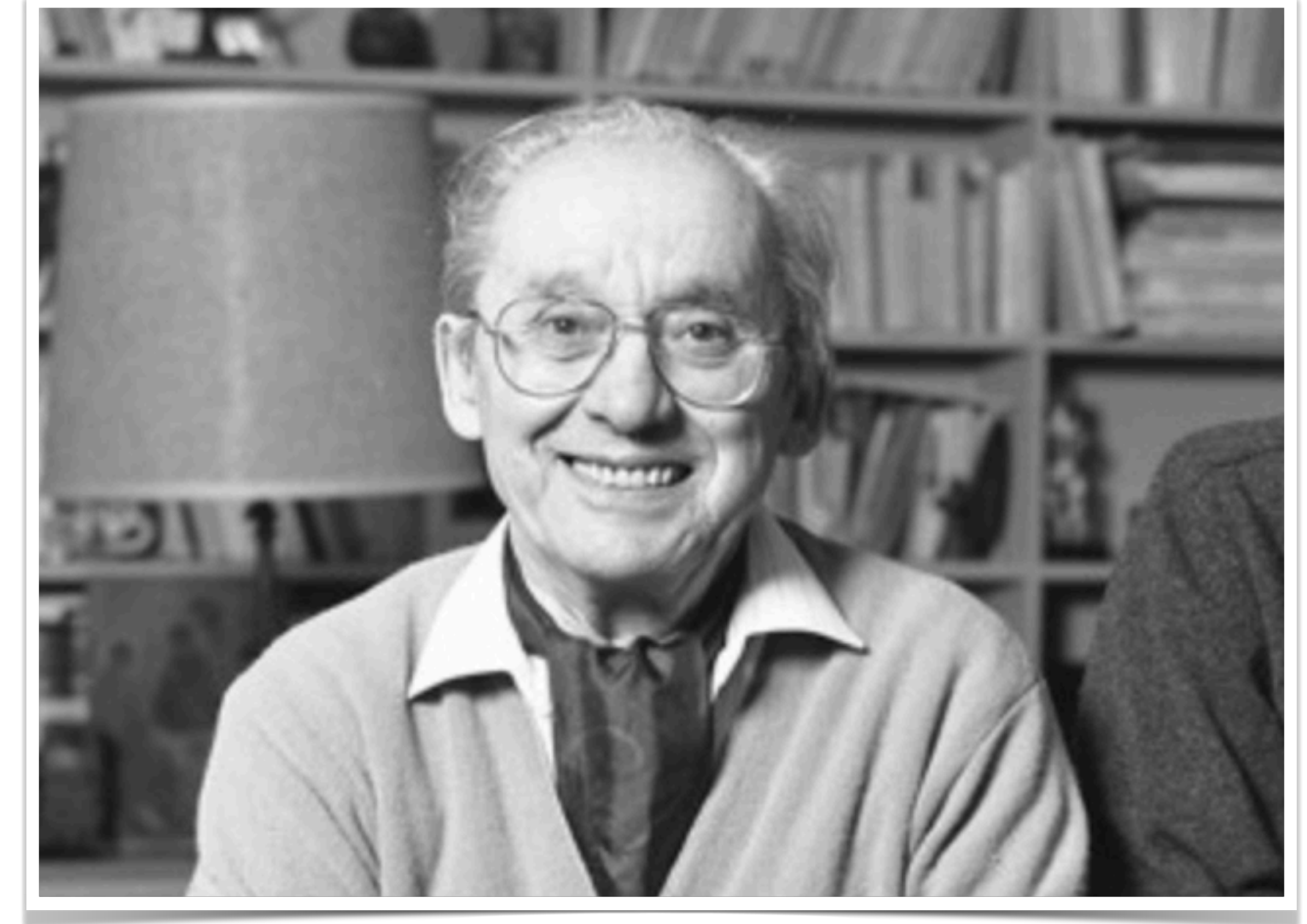
- ▶ Attribution of meaning becomes decisive for **social acceptance or rejection**
 - ▶ Technology futures forge alliances (Ferrari & Lösch, 2017)
 - ▶ Decide on promotion and regulation of the technology (Grunwald, 2019, p. 106)

Deciphering the meanings?

Three perspectives on Technofutures

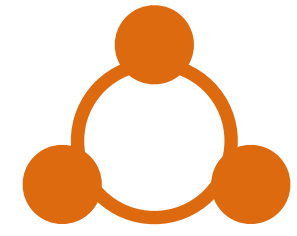
Narrative Hermeneutics

- ▶ **Paul Ricoeur – Time and Narrative (1984)**
- ▶ „Hermeneutics (...) is concerned with reconstructing the entire arc of operations (...) What is at stake, therefore, is the concrete process by which the textual **configuration** mediates between the **prefiguration** of the practical field and its **refiguration** through the reception of the work.“ (Ricoeur 1984, p. 53)

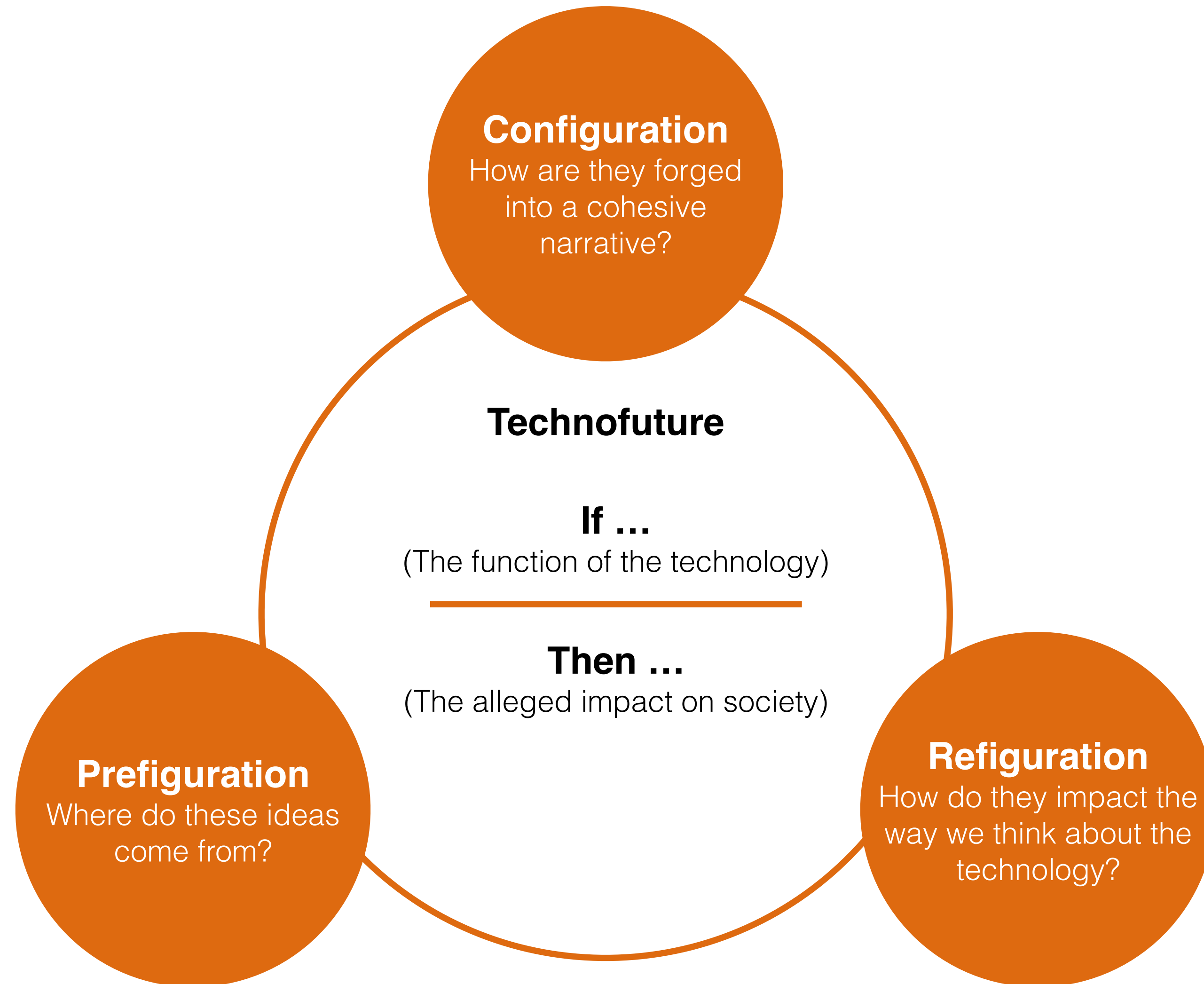


Technofutures as narratives

- ▶ **(1) Prefiguration** Looks at the content of technofutures, how they are entangled in cultural presumptions and informed by culturally shared imaginaries; reflecting on desires, hopes, fears and needs that are inscribed into the respective futures. [**How meaning is drawn from culture**]
- ▶ **(2) Configuration** Looks at the way they are constructed and reflects on the form (e.g., the role of the medium, the performance, the context in which it is embedded), the rhetoric (e.g., the language, narratives and verbal or visual metaphors used), as well as illustrative material (e.g. tables, pictures, movies or other pieces of art). [**How meaning is constructed**]
- ▶ **(3) Refiguration** Focusses on the impact of technofutures and the way they change present discourses or change already established concepts. This perspective includes, among others, the way that stakeholders position themselves towards the proposed future but also how technofutures impact other discourses and diffuse through society. [**How meaning is attributed by others**]

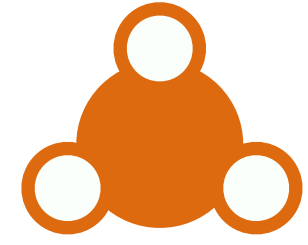


Futures Circle for Hermeneutic TA



Mehnert, W. (2024). The Futures Circle—A Framework for Hermeneutic Technology Assessment. *Technology and Language*, 14(1), 129–151. <https://doi.org/10.48417/technolang.2024.01.10>

Quantum Threat

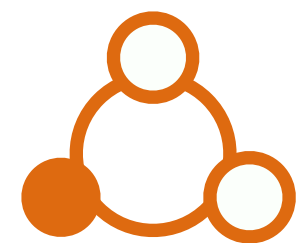


Quantum Threat (Michele Mosca)

The global race to develop quantum computers' has critical implications for cybersecurity. A reliable quantum computer of sufficient size will be able to break some of the most widely used cryptosystems; **hence the notion of Cryptographically-Relevant Quantum Computer (CRQC).** Today's quantum processors are still far from being CRQCs, but the technology is advancing, with no known fundamental barrier, thus making a real CRQC a matter of "when" rather than "if". Those regulating or managing cyber risk should be taking action to address this issue.

▶ Basic Narrative

- ▶ **If** there will be a fully functional [**Cryptographic-Relevant Quantum Computer**] (CRQC), **then** bad actors will misuse it and hack critical data infrastructures
 - ▶ **Variation:** Bad Actors can already collect data today and decrypt it in the future.
 - ▶ **Addition:** To prepare against this risk, it becomes necessary to fund research on [**Post-Quantum-Cryptography**] (PQC) and invest in PQC-infrastructure within companies and governments immediately.



Prefiguration Tech Race Risk

- ▶ **Shor's algorithm** Designed for QCs in 1997 to decrypt standard decryption algorithm (RSA-2048)
- ▶ **Modernization Risk** (Beck, 1986)
 - ▶ „It's a systematic threat to the global economy, and it's real enough that you definitely have to plan for it now.“ (Mosca cited in Mone, 2020)
- ▶ **„Quantum Race“**
 - ▶ technological development as an arms race
 - ▶ e.g. space race, atomic bomb, AI superiority

- Firstly, how long do you need your cryptographic keys to be remain secure? Denote this number by x , the *security shelf-life*. We may have $x = 0$ years for applications requiring only real-time security. Or maybe $x = 10, 20, 100$ years when protecting your personal health information, trade secrets, or national security information. The value of x is in general a personal or business or policy decision.
- Next, how long will it take to deploy a set of tools that are quantum-safe? Denote this number by y , the *migration time*. For example, we may have $y = 0$ years if this is simply a matter of deploying an auto-update that replaces AES-128 with AES-256 within a system fully controlled by a single vendor. However, we may have $y \geq 15$ years if it involves a relatively untested public-key encryption method that has to be adapted for a constrained environment with many players who must agree on a standard.
- Lastly, how long will it be before a quantum computer, or some other method, breaks the currently deployed public-key cryptography tools? Let z denote this number, the *collapse time*.

If $x + y > z$, we have a serious problem today [Mos13], since information protected by quantum-vulnerable tools at the end of the next y years can be broken by quantum attacks in less than x years from then.

Configuration Cryptocalypse (Lindsay, 2020)

▶ Bad Actor Narrative

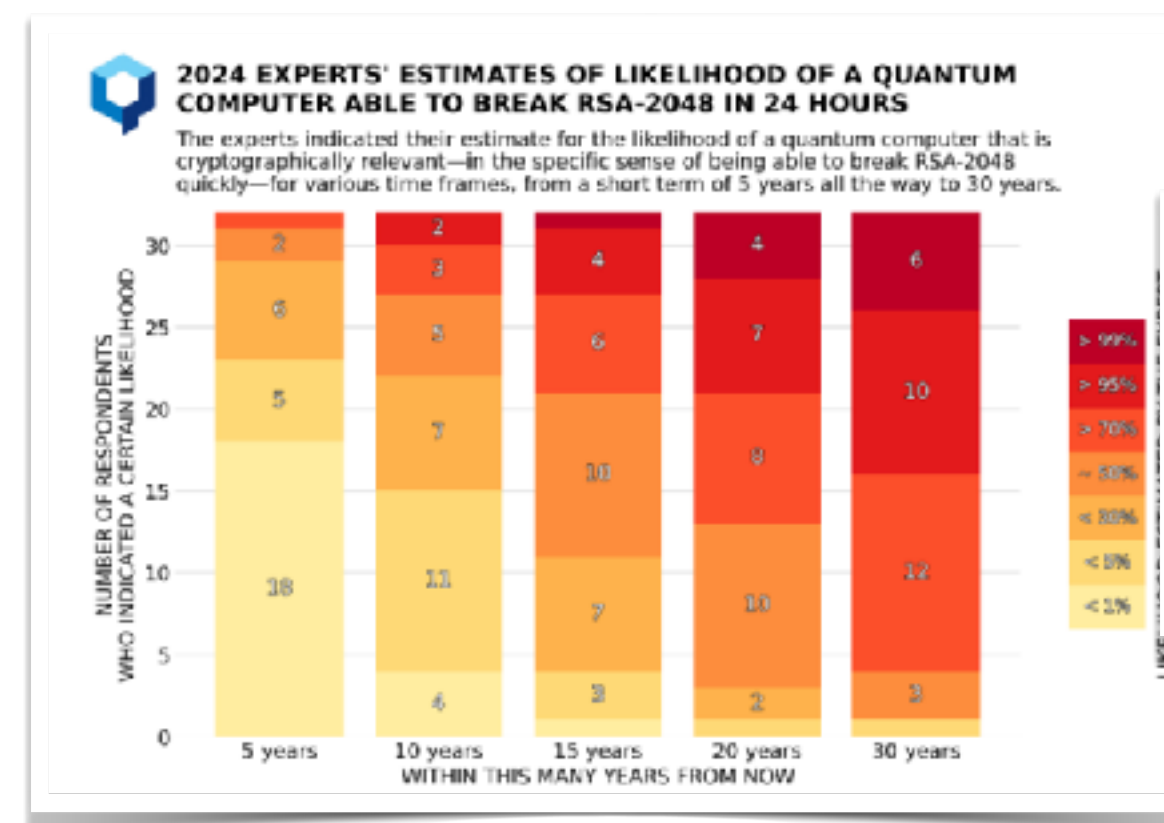
- ▶ Responsibility gets shifted down the innovation chain
- ▶ Basic research > Engineering > mischievous User

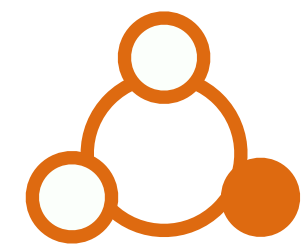
▶ Hype

- ▶ Fear mongering
- ▶ Surveys that ask „when does it happen“, not „if“ or „how likely is it“?
- ▶ *Harvest Now, Decrypt Later* (HNDL attack)

▶ Call to Action Act now or you will regret later

- ▶ „Assess your risk“
- ▶ „Learn how to make your data Quantum Safe with [**Post-Quantum-Cryptography**]“
- ▶ Policy level: „Fund PQC now to protect national / global economy“





Refiguration Policy follows fear mongering

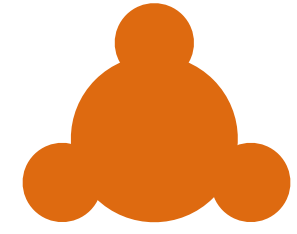
- ▶ „While the **full range of applications** of quantum computers **is still unknown**, (...) quantum computing also poses significant risks to the economic and national security of the United States. Most notably, a quantum computer of sufficient size and sophistication — also known as a [**cryptanalytically relevant quantum computer (CRQC)**] — **will be capable of breaking much of the public-key** cryptography used on digital systems across the United States and around the world.“ (The White House, 2022)
- ▶ Why not a moratorium?

AUGUST 13, 2024

FACT SHEET: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future

PRESS RELEASE | Publication 23 June 2025

EU reinforces its cybersecurity with post- quantum cryptography



Conclusion So what?!

▶ Should I act as a policy maker?

- ▶ The risk is higher than the investment costs, you have to act (Possati, 2023)

▶ Artificial Demand?

- ▶ "According to a long-running joke (or not-quite-joke) in our field, one of the central applications of quantum computing will be to create demand for quantum cryptography!" (Aaronson, 2018)

▶ Technology Mafia

- ▶ „Just look at your beautiful global trade system. It would be a shame, if something happens to it, no?“



Critical Hype Studies

- ▶ **Becoming aware of the construction of Technofutures**
- ▶ Narratives, contexts, purpose, resonance, and more.
- ▶ Sam Altman to the question:
 - ▶ „What keeps you up at night?“
 - ▶ „There’s a bad guy gets [**superintelligence**] and misuses it before the rest of the world has a powerful enough version to defend.“



Wrap Up and Take Away

- ▶ This approach
- ▶ ... structures a hermeneutic technology assessment: (1) Prefiguration, (2) Configuration and (3) Refiguration...
- ▶ ... Reflects the preconceptions, cultural context, desires and hopes – not the technology...
- ▶ ... helps to deconstruct techno-hypes (exaggerations & fear mongering)

Thank you!

- ▶ Mehnert, W. and Grunwald, A. (2024): **Hermeneutic Technology Assessment**. In: Grunwald, A. (ed.): International Handbook of Technology Assessment. London: Edward Elgar Publishing (in press).
- ▶ Mehnert, W. (2024). **The Futures Circle—A Framework for Hermeneutic Technology Assessment**. Journal of Technology and Language, Special Issue on Hermeneutics of Technology, 14(1), 129–151.

Wenzel Mehnert

mail@wenzelmehnert.de



